An efficient and Automatic Algorithm for Image Forgery Detection

M.Srujana[1], Ch.Anuradha[2], Patnala S.R. Chandra Murty[3]
[1]*Student, CSE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*
[2]*Research Scholar, CSE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*
[3]*Assistant Professor, CSE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*

Abstract- **With the development of sophisticated image editing and manipulation tools, the originality and authenticity of a digital image is usually hard to determine visually. In order to detect digital image forgeries, various kinds of digital image forensics techniques have been proposed in the last decade. Compared with active forensics approaches that require embedding additional information, passive forensics approaches are more popular due to their wider application scenario, and have attracted increasing academic and industrial research interests. A novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and key point-based forgery detection methods. First, the proposed Adaptive Over-Segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labelled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we proposed, the Forgery Region Extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighbouring blocks that have similar local colour features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy-move forgery detection methods.**

Index terms- Forgery Detection, Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction

I. INTRODUCTION

Image forgery has been an issue since the advent of traditional photography in the 19th century; however it is a much more prevalent problem in the digital age. The primary issue is that photographs are often used as concrete evidence of an event, and are generally seen by the public as truthful and trustworthy. Images that are forged, therefore abusing this trust, can have many wide-reaching social impacts.

With the development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. In recent years, more and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into other part(s) of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case.

The organization of the paper is as follows: Section 1 gives an introduction, Section 2 covers earlier research in Image forgery detection and Section 3 presents proposed methodology. Section 4 covers computational results and discussion, followed by summary of research in Section 5.

II. RELATED WORK

In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature keypoint-based algorithms. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients.

Fridrich et al. Proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid applied Principal Component Analysis (PCA) to reduce the feature dimensions. Luo et al. used the RGB color components and direction information as block features. Li et al. used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic calculated the 24 Blur-invariant moments as features. Kang and Wei calculated the singular values of a reduced-rank approximation in each block. Bayram et al. used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. [8, 9] used the mean intensities of circles with different radii around the block center to represent the block features. Lin et al. used the gray average results of each block and its sub-blocks as the block features. Ryu et al. used Zernike moments as block features.

Bravo-Solorio and Nandi used information entropy as block features. As an alternative to the block-based methods, keypoint-based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In, the Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In, the Speeded Up Robust Features (SURF) were applied to extract features instead of SIFT.

However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate. Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing keypoint-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor.

III. PROPOSED WORK

This section describes the proposed image forgery detection using adaptive over-segmentation and feature point matching in detail. First, an adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks called Image Blocks (IB). Then, we apply the Scale Invariant Feature Transform (SIFT) in each block to extract the SIFT feature points as Block Features (BF). Subsequently, the block features are matched with one another, and the feature points that are successfully matched to one another are determined to be Labeled Feature Points (LFP), which can approximately indicate the suspected forgery regions. Finally, we propose the Forgery Region Extraction method to detect the forgery region from the host image according to the extracted LFP. In the remainder of this section, Section II-A explains the proposed Adaptive Over-Segmentation method in detail; Section II-B introduces the Feature Point Extraction using SIFT; Section II-C describes the Block Feature Matching procedures; and Section II-D presents the proposed Forgery Region Extraction method.

After we have obtained the block features (BF), we must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks. Fig. 5 shows the flowchart of the Block Feature Matching algorithm. First, the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is calculated adaptively; with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region. The detailed steps are explained as follows.

Algorithm: Block Feature Matching algorithm

Input: Block Features (BF);

Output: Labelled Feature Points (LFP).

STEP-1: Load the Block Features BF = {BF1, BF2,BFN....., }where N means the number of image blocks; and calculate the correlation coefficients CC of the image blocks.

STEP-2: Calculate the block matching threshold BTR according to the distribution of correlation coefficients.

STEP-3: Locate the matched blocks MB according to the block matching threshold B TR.

STEP-4: Label the matched feature points in the matched blocks MB to indicate the suspected forgery regions.

IV. RESULTS AND DISCUSSION

Use either SI (MKS) or CGS as primary units. (SI Using the Adaptive Over-Segmentation method described above, in Fig. 1-(A1), the size of the host image I1 is M1xN1=1632x1224 ; according to (1), PLF_1 can be calculated, as PLF_1=50.19% ; therefore, the adaptive initial size of the superpixels is calculated using (4), which yields S _1=199 . Similarly, for the host image I2 in Fig. 32-(B1), with the size M2xN2 =1306x1950, PLF_2 =39.89%, and S _ 2 =159; for the host image I3 in Fig. 3.4-(C1), with the size M3xN3 =1936x1296, PLF_ 2= 59.92%, and S _3= 224. Fig. 1-(A4), (B4), and (C4) show the host image segmentations with the proposed Adaptive Over-Segmentation method, and (a4), (b4), and (c4) show the corresponding detected forgery regions with the proposed Adaptive Over-Segmentation method. We can see that in Fig.2-(A), with the calculated adaptive size, S_1=199, the forgery detection result in Fig. 2-(a4) performs better than the results when the fixed sizes are S=150 and S=250 (which are given in Fig. 1-(a2) and (a3), respectively). In Fig. 4-(B), with the calculated adaptive size S_2=159, the forgery detection result in Fig. 2-(b4) is similar to the result in Fig. 4-(b2) when S=150; in addition, it performs better than the results in Fig. 1-(b3) when S=250. In Fig. 1-(C), with the calculated adaptive size, S_ 3= 224, the forgery detection result in Fig. 1-(c4) becomes close to the result in Fig. 2-(b3) when S=250, and it performs better than the results in Fig. 2-(b2) when S=150 .

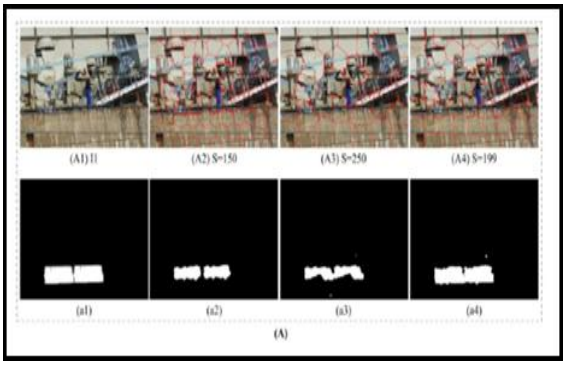

Fig 1 Detecting forgery regions with the proposed Adaptive Over-segmentation method

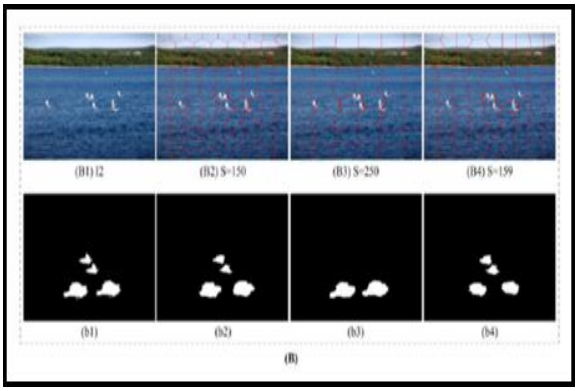

Fig 2 Super pixels of different initial sizes and the corresponding forgery detection results

Fig 3.4 Super pixels of different initial sizes and the corresponding forgery detection results (A1), (B1), and (C1). The copy-move host images, I1, I2 and I3;

(a1), (b1), (c1) the corresponding forgery regions of I1, I2 and I3, respectively. (A2), (B2), (C2) the host images are blocked into super pixels with initial size S 150; (a2), (b2), (c2) the corresponding detected forgery regions when S 150. (A3), (B3), (C3) the host images are blocked into super pixels with initial size S 250; (a3), (b3), (c3) the corresponding detected forgery regions when S 250. (A4), (B4), (C4) The host images are blocked into super pixels with the proposed Adaptive Over-segmentation method, by which the initial super pixel sizes are calculated as 199 S , 159 S , and 224 S , respectively; (a4), (b4), (c4) The corresponding detected forgery regions with the proposed Adaptive Over-segmentation method. As discussed above, the proposed Adaptive Over-Segmentation method can divide the host image into blocks with adaptive initial sizes according to the given host images, with which each image can be determined to be an appropriate block initial size to enhance the forgery detection results. The proposed Adaptive Over-Segmentation method can lead to better forgery detection results compared with the forgery detection methods, which segment the host images into fixed-size blocks and, at the same time, reduce the computational expenses compared with most of the existing forgery detection methods, which segment the host images into overlapping blocks.

V. CONCLUSION

The copy-move forgery detection is one of the emerging problems in the field of digital image forensics. Many techniques have been proposed to address this problem. One of the biggest issues these techniques had to deal with was, being able to detect the duplicated image regions without getting affected by the common image processing operations, e.g. noise adding and blurring. The other challenge was computational time, which becomes important considering the large databases; these techniques would be used on. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labelled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labelled feature points are replaced with small super pixels as feature blocks, and the neighbouring feature blocks with local colour features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions. We demonstrate the effectiveness of the proposed scheme with a large number of experiments. Experimental results show that the proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling, compared with the existing state-of-the-art copy-move forgery detection schemes. Future work could focus on applying the proposed forgery detection scheme based on adaptive over-segmentation and feature-point matching on other types of forgery, such as splicing or other types of media, for example, video and audio.

ACKNOWLEDGMENT

The authors like to convey regards to the editor for consideration of this manuscript and also for suggestions and comments from anonymous referees which are very helpful to improve both quality and presentation of this research paper.

REFERENCES

[1] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, “A sift-based forensic method for copy-move attack detection and transformation recovery,” IEEE Trans. on Information Forensics and Security, vol. 6, no. 3, pp. 1099-1110, 2011.

[2] P. Kakar and N. Sudha, “Exposing post-processed copy-paste forgeries through

transform-invariant feature," IEEE Trans. on Information Forensics and Security, vol. 7, no. 3, pp. 1018-1028, June 2012.

[3] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750-1753.

[4] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2007.

[5] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.

[6] X. Pan, S. Lyu," Detecting image region duplication using SIFT features", in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), 2010, 2010, 1706–1709.

[7] Frank Y. Shih and Yuan Yuan, "A Comparison Study on Copy-Cover Image Forgery Detection", The Open Artificial Intelligence Journal, 2010, 4, 49-54.

[8] Preeti Yadav, YogeshRathore, Aarti Yadav," DWT Based CopyMove Image Forgery Detection", International Journal of Advanced Research in Computer Science an Electronics Engineering Volume 1, Issue 5, July 2012

[9] Hwel-Jen Lin, Chun-We Wang," Fast Copy-Move Forgery Detection", WSEASTransactions on SIGNAL PROCESSING, May 2009.